VIACCESS DATA PROTECTION POLICY

PREAMBLE

The General Data Protection Regulation (GDPR) sets out the legal framework for the handling of personal information that identifies living people. All organisations holding or processing personal data must comply with the Regulation as of 25th May 2018. This Data Protection Policy is to assist in managing and processing personal data in accordance with the GDPR. It is essential that you read and understand this Data Protection Policy and what is required of you.

INTRODUCTION

This Data Protection Policy is our commitment to treat personal information of employees, customers, stakeholders and any other interested parties with the utmost care and confidentiality because everyone has rights with regard to the way their personal data is handled. The aim of this Data Protection Policy is to ensure that we at VIACCESS collect, store and handle personal data fairly, transparently and with the greatest respect to individual rights. We recognise the need to treat their personal data in an appropriate and lawful manner.

SCOPE

All employees at VIACCESS and its subsidiaries must observe this Data Protection Policy at all times. Contractors, consultants, partners and any other external entity are also concerned. In general, this Data Protection Policy applies to anyone we collaborate with or acts on our behalf and may need occasional access to Personal data.

Personal data is defined as:
«**Any information relating to** an identified or identifiable **natural person** ('data subject'); an identifiable natural **person is one who can be identified, directly or indirectly**, in particular by reference to an identifier such as **a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person» Art 4.1 GDPR**

Personal data includes personal information that identifies a living individual such as names, addresses, telephone numbers, IP addresses, mobile phone numbers, personal email addresses, dates of birth, bank details, employment history/CV, passport information, payroll information, performance review, usage data (such as TV viewing habits, smartphone), data that identifies current, past and prospective employees, contractors, suppliers, customers, and others with whom VIACCESS conducts business or otherwise communicates with. Personal data also includes personal information that *indirectly* identifies individuals, such as pseudonymized data. This Data Protection Policy applies to our customers' customers data which we process, whether or not our customers' customers are directly or indirectly identified or identifiable. In this context, VIACCESS may be acting as both, **Data Controller**, processing data for its own purpose (e.g. HR data) and as **Data Processor**, processing data on behalf of its customers. When acting as Data Controller, VIACCESS determines the purpose for which and the manner in which any personal

data is, or is to be processed. When acting as Data Processor, VIACCESS follows the processing instructions provided by its customers as contractually agreed with such customers.

OUR COMMITMENT

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, bank details and so on.

VIACCESS is committed to collect this information in a transparent manner and only with the full cooperation and knowledge of interested parties. Once this information is available to us, we observe the following rules.

Personal data must be:

- accurate and kept up-to-date
- collected fairly and for solely for lawful purposes
- processed in accordance with the GDPR
- protected against any unauthorised or illegal access by internal or external parties

Personal data must not be:

- communicated informally
- stored for more than a specified amount of time
- transferred to organisations, states or countries which do not have adequate data protection policies and safeguard measures. Countries providing an adequate level of data protection are listed in the so called “white list" at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
- distributed to any party other than the ones agreed upon by the data controller (exempt for a legitimate request from a law enforcement authority)

In addition to the manner we handle personal data, we have obligations to the individuals to whom the data relates to.

Specifically we must tell the individuals:

- what of their personal data is collected
- how long we keep their personal data
- who has access to their personal data
- what security measures are in place to ensure the safety of their personal data
- what procedure is in place to allow them to modify, erase, reduce or correct their personal data contained in our databases

We are committed to:

- restrict and monitor access to personal data
- develop transparent data collection procedures
- train employees accordingly
- build secure networks to protect online data from cyber attacks
- establish clear procedures for reporting personal data breaches

- Include contract clauses or communicate statements on how we handle personal data
- establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorisation)
- Our Data Protection Policy is indicated on our website

LAWFUL PROCESSING

Processing is defined as:
«**Any operation or set of operations** which is performed on personal data or on sets of personal data, **whether or not by automated means**, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction» Art 4.2 GDPR

WHAT ARE OUR OBLIGATIONS?

The GDPR sets key principles regarding the processing of personal data as summarised in the tables below.

When acting as Data Controller, our obligations are as follows:

1	**PURPOSE**	**DEFINE THE PURPOSE OF THE FILE** Before any collection and use of personal data, the data controller must inform the people concerned how he will use their data. This is the "purpose", which must respect the rights and freedoms of individuals. It limits how the controller can use or reuse the data in the future. = principle of lawfulness, fairness and transparency
2	**RELEVANCE**	**CHECK THE RELEVANCE OF THE DATA** Only data strictly necessary for achieving the purpose must be collected: this is the principle of data minimisation. The controller should not collect more data than he needs. He must also pay attention to the sensitive nature of certain data.
3	**STORAGE**	**STORAGE LIMITATION OF DATA** Once the purpose of data collection is achieved, there is no longer a need to keep the data and it must be deleted. This storage period must be defined in advance by the controller whilst observing any obligation to retain certain data**.**
4	**RIGHTS**	**RESPECT THE RIGHTS OF INDIVIDUALS** Data concerning individuals can be collected on condition that they have been informed of the operation. These individuals have certain rights that they can exercise before the organisation that holds the data concerning them: a right to access the data, a right to rectify it and finally a right to oppose to their use.
5	**SECURITY AND CONFIDENTIALITY**	**SECURITY AND CONFIDENTIALITY OF THE DATA** The data controller must take all necessary measures to ensure the security of the data he has collected but equally their confidentiality to ensure that only authorised personnel have access to it. These measures can be determined according to the risks weighing on this file (sensitivity of the data, purpose of the processing ...). The data controller must use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in order to ensure the security and the confidentiality of the data.

6	**DATA BREACH**	**NOTIFICATION OF DATA BREACH** A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. Any Data Breach or suspicion thereof must be reported **immediately** after being detected to our Chief Security Officer (Quentin CHIEZE, Quentin.CHIEZE@viaccess-orca.com), the General Counsel and Security (Christine Maury Panis, Christine.MAURY-PANIS@viaccess-orca.com) and our DPO (Emmanuel Cauvin, dpo@viaccess-orca.com) for further action.
7	**ACCOUNTABILITY & RECORD KEEPING**	**RESPONSIBILITY** The data controller is responsible for compliance with the GDPR and must be able to demonstrate compliance. In which case, the data controller must maintain a record of processing activities under its responsibility ("VIACCESS' Data Controller Register").

When acting as Data Processor, our obligations are as follows:

1	**PURPOSE**	The purpose of the data processing is defined by the data controller, i.e. VIACCESS' customers. It is an obligation for the data processor to use the data solely as defined by the data controller. The data processor must Not in any case whatsoever use the data for its own purpose.
2	**RELEVANCE**	**NOT APPLICABLE HERE, ASSUMING THE DATA PROCESSOR IS NOT COLLECTING DATA DIRECTLY FROM THE DATA SUBJECTS.**
3	**STORAGE**	**STORAGE LIMITATION OF DATA** The data processor must not keep the data longer than the duration defined in the contract signed with the data controller**.**
4	**RIGHTS**	**RESPECT THE RIGHTS OF INDIVIDUALS** The data processor must support the data controller when individuals exercise their rights, in accordance with the contract signed between the two parties.
5	**SECURITY AND CONFIDENTIALITY**	**SECURITY AND CONFIDENTIALITY OF THE DATA** The data processor must take all necessary measures to ensure the security of the data he has collected but equally their confidentiality to ensure that only authorised personnel have access to it. These measures are often determined in the contract signed with the data controller, i.e. VIACCESS' customers. The data processor must use only sub-processors providing sufficient guarantees to implement appropriate technical and organisational measures in order to ensure the security and the confidentiality of the data.
6	**DATA BREACH**	**NOTIFICATION OF DATA BREACH** A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. Any Data Breach or suspicion thereof must be reported **immediately** after being detected to our Chief Security Officer (Quentin Chieze, Quentin.CHIEZE@viaccess-orca.com), the General Counsel and Security (Christine Maury Panis, Christine.MAURY-PANIS@viaccess-orca.com) and our DPO (Emmanuel Cauvin, dpo@viaccess-orca.com) for further action.
7	**ACCOUNTABILITY & RECORD KEEPING**	**RESPONSIBILITY** The data processor is responsible for compliance with the GDPR and must be able to demonstrate compliance. In which case, the data processor must maintain a record of processing activities carried out on behalf of its customers ("VIACCESS' Data Processor Register").

Therefore to lawfully process personal data certain conditions must be observed.

We must ensure that the personal data we collect and use is:

- kept safe at all times and that not anybody can have access to the data
- used only for the purpose for which it was collected
- used by you properly when performing your normal work duties
- is accurate and kept up to date
- kept no longer than necessary and disposed of in a correct and safe manner
- always obtained with the express consent of the individual concerned or
- that the processing is necessary for a legitimate interest of the individual or the party to whom the personal data is disclosed, such as for payroll reason.

VIACCESS POLICY STATEMENT

It is VIACCESS Policy to:

- only collect, handle, process, store, record, use, transport, and retain personal data that is necessary for the Company to conduct its business
- respect the privacy of individuals
- ensure that any personal data held is secure, giving access only to those who have a lawful right to access whether automated or manual records.

Every employee or worker at VIACCESS has a duty to adhere to VIACCESS' Data Protection Policy. Anyone managing a Personal Data Processing has key responsibilities for the implementation, application and monitoring of this Data Protection Policy. If you are unsure about how you should apply or interpret this Data Protection Policy, or are concerned about a possible breach, you should check with your line manager or contact our Data Protection Representatives (Christine Maury Panis, Marie-Odile Landerneau or Quentin Chieze) for guidance prior to taking any action. Additionally, we have a Data Protection Officer ("DPO") whom be reached at dpo@viaccess-orca.com.

This Data Protection Policy may be amended at any time. **Any breach of this** Data Protection Policy **will be taken seriously and may result in disciplinary action**.

Date of creation: 2018
Updated: